In yet another example, a fingerprint or retinal scan is used as the lockout bypass input. The step of receiving 110 in this example comprises performing and digitizing a fingerprint or retinal scan. The step of comparing 120 comprises comparing the digitized fingerprint or retinal scan to a stored fingerprint or retinal scan template of the authorized user. If the step of comparing 120 produces a match between the digitized scan and the template, the lockout bypass input is considered to be valid. If a match is not produced, the lockout bypass input is not valid. The term 'match' as used herein includes an identical or 1:1 match or an unambiguous correspondence between the input and the template.

In yet another example, the user transmits a coded message or signal to the device using an RF or IR transmitter. The coded signal in this case is the lockout bypass input. In this example, the step of receiving 110 may comprise transmitting the signal. The step of receiving 110 further comprises receiving the transmitted signal. In the step of comparing 120, the received signal or a representation of the received signal is compared to a representation or template of the signal stored in memory. As in the other examples, if the comparison 120 produces a match therebetween, the lockout bypass input is considered to be valid. If a match is not produced, the lockout bypass input is not valid. The above-referenced examples of various bypass lockout inputs of the step of receiving 110 are provided by way of example and are not intended to limit the scope of the present invention.

In a preferred embodiment, a lockout bypass is received 110 and compared 120 during a start-up process of the device. The device performs the start-up process each time the device is turned 'ON'. Preferably, at some point during start-up, the device halts the start-up process and waits for a lockout bypass input. The device can wait indefinitely until a lockout bypass is received 110. More preferably, if a lockout bypass is not received 110 within a predetermined period of time, the lockout bypass is considered invalid. In addition, the step of receiving 110 may be repeated one or more times when an invalid lockout bypass is received, or when no input is received, to account for input errors and input time delays on the part of the user.

Once a valid lockout bypass is received 110, the device need not receive 110 another lockout bypass input until a next start-up process. Thus in some

embodiments, once a lockout bypass is received 110, the device must be turned 'OFF' and back 'ON' before the steps of receiving 110 and comparing 120 are repeated. In other alternative embodiments, the steps of receiving 110 and comparing 120 the lockout bypass input may be performed at times either in addition to or other than during the start-up process, and even be repeated periodically during device operation following completion of the startup process. For example, the steps of receiving 110 and comparing 120 the lockout bypass input may be repeated approximately every 20 to 30 minutes during device operation, or at other time intervals. The alternative embodiments enable the device employing method 100 to periodically 'check' to see if an authorized user is still using the device. In this way, an authorized user who loses the electronic device after the valid lockout bypass input is received still can realize the benefits of the present invention.

The method 100 further comprises disabling 130 the device if or when an invalid lockout bypass is received 110. Once the step of comparing 120 has determined the lockout bypass input to be invalid, normal operation of the device is disabled 130. However, if the step of comparing 120 determines that a valid lockout bypass is received 110, the device is enabled instead of being disabled and operates normally. When enabled during start-up, the device can continue the start-up process. Once start-up is completed, the device becomes operational. If the security bypass lockout is requested during operation, the device can continue normal operation upon receipt of the correct bypass lockout input.

With reference to the password example above, if an incorrect password is input by the user during the start-up process or at other requested times, the device is disabled 130. Preferably, the device begins a shutdown process when disabled 130. Thus, the device turns itself 'OFF' if an invalid password is entered by the user, thereby effectively denying use to a user who does not have the correct password.

The method further comprises displaying 140 owner information if an invalid lockout bypass is received 110. The owner information is displayed preferably using the user interface of the device. For example, the owner information can be displayed on an alphanumeric display of the device.

The owner identification may include a name of an owner and may optionally include owner contact information. For example, the name and address and/or telephone number of the owner can be displayed. Alternatively, the owner information displayed may be contact information for a lost and found service. In addition to owner information, a message indicating that security lockout is active can be displayed to let a user know why the device is not functioning. Preferably, the step of displaying 140 is performed following each time an invalid lockout bypass is received 110. In general, return-to-owner information includes, but is not limited to, one or more of a name for the owner, an address for the owner, a telephone number for the owner, return-to-owner instructions, a device serial number, a name for a lost and found service, an address for the lost and found service, a telephone number for the lost and found service, lost and found service return instructions, return to manufacturer instructions, and return to law enforcement office instructions.

If the displayed owner information includes an address and/or telephone number for the owner, the owner can be contacted directly and the device can be returned directly to the owner. For example, a Good Samaritan finding the device can use the address to mail the device back to the owner. Likewise, a law enforcement agency recovering the device can contact the owner directly using the displayed address/telephone information. Alternatively, the device can display 140 a message that postage is guaranteed by a lost and found service along with the lost and found service address or contact information. In addition, a monetary reward or other inducement to return the device may be offered by the owner or the lost and found service as a means to encourage the return of the device. A reward announcement may be displayed along with the owner information.

Depending on the device, the display 140 of owner information can be momentary or continuous. A momentary display preferably lasts long enough for the information being displayed to be read and understood. Typically, one to five minutes is a sufficient display duration for such a momentary display of owner information. When the device begins a shutdown process after being disabled 130, the owner information is displayed 140 momentarily only for two minutes, for example. The use of a momentary display 140 of the owner information is usually for